

REMARKS

This Response is submitted in response to a final *Office Action* mailed February 20, 2008. Claims 1-17 are pending in the application. Claim 4 is rejected under 35 U.S.C. § 112, first paragraph for allegedly failing to comply with the written description requirement. Claims 1, 2, and 5-17 stand rejected under 35 U.S.C. § 102(e) as allegedly anticipated by U.S. Publication No. 2003/0221123 A1 to Beavers (hereinafter "Beavers"). Claims 3 and 4 stand rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over Beaver in view of *Best Practices in Network Security* by Frederick M. Avolio (hereinafter "Avolio").

Applicants have amended claim 1 and added claim 20. The amendments above add no new subject matter. Support for the amendments may be found in the original specification and claims.

Applicants respectfully traverse the Examiner's rejections and request reconsideration of the claims in light of the amendments above and remarks below.

I. Claim 4.

Claim 4 is rejected under 35 U.S.C. § 112, first paragraph for allegedly failing to comply with the written description requirement. While service values are not described in the description of threshold provided in paragraph 69 of the specification, service values are described throughout the specification and used in the same general context as node values. See, e.g., Figure 3. The description of "threshold" in paragraph 69 is merely one example of a threshold and its relation to a node value. Thresholds can be associated with other values.

Since service values and node values are described in the same context, it would be clear to one of skill in the art that the threshold could be related to a service value. Explicit support for a service value-related threshold can be found, for example, in paragraph 41, which describes comparing a threat level to both a node value threshold (nodeThreshold) and a service value threshold (serviceThreshold). One of skill in the art would understand based on the specification that the threshold could be compared to either of these values. Thus, Applicants respectfully request that the Examiner withdraw the rejection of claim 4.

II. Claims 1, 2, 5-17.

Claims 1, 2, 5-17 stand rejected under 35 U.S.C. § 102(e) as allegedly anticipated by U.S. Publication No. 2003/0221123 A1 to Beavers (hereinafter “Beavers”). In order to anticipate a claim under 35 U.S.C. § 102(b), a reference must teach each and every element of a claim. *See* MPEP § 2131.

Respectfully, Beavers does not teach each and every element of the rejected claims. In claim 1, Applicants claim “an authorization enforcement facility...operable to perform a risk-aware analysis of [a] connection to determine [a] threat level associated with the connection based at least in part on the static policy data attribute, and store the determined threat level in the dynamic policy data store as a dynamic policy data attribute.” Beavers does not disclose a “an authorization enforcement facility...operable to perform a risk-aware analysis of [a] connection to determine [a] threat level associated with the connection based at least in part on the static policy data attribute, and store the determined threat level in the dynamic policy data store as a dynamic policy data attribute.”

The system disclosed in Beavers receives as input security events or “alerts” that are generated by devices that monitor security-related threats. The system produces an incident declaration as output. *See, Beavers*, ¶¶ 3, 9-11. The purpose of the system in Beavers is to filter alerts in a network to alleviate the burden on an overworked security administrator. *See, Beavers*, ¶ 4. To achieve this, Beavers' processes alerts by matching them against a set of rules to exclude low-priority alerts (*See, Beavers*, ¶13) and false positives (*See, Beavers*, ¶ 82), thus only declaring “high-quality” incidents. The system in Beavers uses two types of decision tables in analyzing alerts, a correlation decision table and a watch list decision table. *See, Beavers*, ¶¶ 44, 48. The correlation decision table is a user-defined spreadsheet that allows a user to define a pattern of interest and a corresponding response. *See, Beavers*, ¶¶ 46, 49. The watch list decision table contains “information that should be remembered for possible incident declarations as further significant alerts are received;” it is essentially a buffer. *See, Beavers*, ¶ 44. By default, it is constructed automatically based on the correlation decision table, but may also be edited by the user to override the automated construction. *See, Beavers*, ¶ 52.

Beavers describes a set of static rules for examining alerts that have been triggered and determining that those alerts are false positives. *See, e.g., Beavers*, Figures 3 and 5. Similarly,

customer-specific enterprise rules are used in Beavers' IM.rules file, which is used to reduce false positives when declaring incidents, not to perform risk analysis. *See, Beavers*, ¶ 73. For instance, Beavers states, "ACME CORP. POLICY IMPLEMENTATION: Declare an incident if you get ANY alert from a source that is on the bad guy list (or add to an existing incident, which is what DECLARE_STANDARD_INCIDENT does if the alert tracks to an existing incident)." *Beavers*, ¶ 84.

Beavers describes two types of decision tables – a correlation decision table and a watch list decision table. *See, Beavers*, ¶¶ 44, 48. The correlation decision table is a user-defined spreadsheet that allows the user to specify how to discern patterns that are of interest, and whether to respond to such patterns by declaring an incident. *See, Beavers*, ¶ 46, 47. Each row in the correlation decision table represents an incident signature that is defined by the user. *See, Beavers*, ¶ 52.

These characteristics differ from the subject matter of claim 1 in a number of ways. First, as described above, the stated objective of Beavers' correlation decision table is to declare incidents, which again are meant to alleviate the burden on an overworked security administrator. In contrast, in claim 1, applicants claim an authorization enforcement facility operable to perform "a risk-aware analysis of the connection to determine the threat level associated with the connection." Further, Beavers' correlation decision table is statically defined by the user. *See, Beavers*, ¶ 4. In contrast, in claim 1, Applicants claim an automated enforcement facility operable to "store the determined threat level in the dynamic policy data store as a dynamic policy data attribute."

In addition, Beavers' correlation decision table stores a set of incident signatures. *See, Beavers*, ¶ 52. In contrast, in claim 1, applicants claim "a dynamic policy data store for tracking a threat level associated with a connection."

Beavers' second decision table, the alert watch list decision table, acts as a "buffer" to remember alert information as the system receives alerts for processing. *See, Beavers*, ¶ 52. The watch list can be edited manually, though by default it is built automatically using information in the Correlation Decision Table for the benefit of less experienced users. *See, Beavers*, ¶ 52. Similar to the correlation decision table, the intent of the alert watch list is also to examine whether incidents should be declared.

These characteristics differ from the dynamic policy data store claimed in claim 1 in several ways. For instance, Beavers' watch list is derived from a static correlation decision table. *See, Beavers*, ¶ 54. In contrast, in claim 1, Applicants claim an authorization enforcement facility operable to "store the determined threat level in the dynamic policy data store as a dynamic policy data attribute." Also, Beavers' alert watch list may be overridden by the user. *See, Beavers*, ¶ 52. In contrast, in claim 1, the authorization enforcement facility is operable to "store the determined threat level in the dynamic policy data store as a dynamic policy data attribute." Further, Beavers' alert watch list table identifies the information that should be remembered for possible incident declarations. *See, Beavers*, ¶ 44. In contrast, in claim 1, Applicants claim "a dynamic policy data store for tracking a threat level associated with a connection."

Beavers' also describes a dynamic threat table and a dynamic tracking table. The dynamic threat table is apparently used to store remembered information from the watch list. *See, Beavers*, ¶ 54. Beavers provides very little information about the dynamic threat table, other than that it is an internal data structure that is not seen or accessed by the user and it stores one row per network asset. *See, Beavers*, ¶ 54. While it is likely an internal data structure that is used to support the implementation of the alert watch list, Beavers does not provide sufficient disclosure to compare the dynamic threat table with the elements of claim 1.

Beavers' dynamic tracking table is only used after an incident ticket has already been declared. The dynamic tracking table is used to keep "tracking rules," which specify conditions that need to occur before new alerts are appended to the incident ticket. *See, Beavers*, ¶ 94. Beavers only mentions the term "dynamic tracking table" once, stating that the tracking rules are kept in a dynamic tracking table. *See, Beavers*, ¶ 98. No further details are provided as to how the dynamic tracking table actually stores the tracking rules.

For at least these reasons, claim 1 is patentable over Beavers, and Applicants respectfully request that the Examiner withdraw the rejection of claim 1.

Claims 2, 5, and 8-12 depend from and further limit claim 1. Thus, claims 2, 5, and 8-12 are patentable over Beavers for at least the same reasons as claim 1. Applicants respectfully request that the Examiner withdraw the rejection of claims 2, 5, and 8-12.

In claim 6, Applicants claim “[t]he network security system of claim 1, wherein the AEF is further operable to generate a response to the connection.” And in claim 7, Applicants claim “[t]he network security system of claim 6, wherein the response comprises at least one of blocking the source of the connection from connecting to an intended destination, altering the intended destination of the connection, or auditing the connection.”

Beavers does not teach or suggest the limitations of claims 6 and 7. As the Examiner points out, Beavers’ does describe shutting down a web server that is suspected of being compromised. *See, Beavers*, ¶ 39. However, this shutdown occurs only after an incident ticket is declared manually. Further, many different machines could potentially access the web server, while only a subset of those attempting access may be malicious machines intending to compromise the web server. Shutting down the web server automatically would not only prevent those malicious machines from accessing the web server; it would also prevent legitimate machines from connecting as well. Thus, this process differs markedly from “blocking the source of said connection” as claimed in claim 7. In the process as claimed, the AEF blocks the malicious machine from connecting to the web server, such that the malicious machine itself is blocked. Non-malicious machines are still allowed to connect. Furthermore, the web server in Beavers’ is the destination of the connection, not the “source of said connection.”

Beavers' invention also describes diverting information if noise is detected. *See, Beavers*, ¶ 33. According to Beavers, an example of such noise would be legitimate and routine automated probes that are applied by third-party network management and other systems – i.e. events that are of no interest to the security administrator. *Id.* Thus, Beavers diverts this information because it is unwanted and/or unimportant. In contrast, in claim 7, the AEF “perform[s] a risk-aware analysis of the connection to determine the threat level associated with the connection” and then may respond by “altering the intended destination of the connection.” Since the connection has caused an alert, that signifies that the connection may be malicious in some way. Therefore, in order to restrict damage to the end destination, the AEF is “altering the destination of that connection” to lessen the potential for harm to the original destination. In other words, Beavers' diverts information to reduce false positives, where as Applicants claim “altering the destination of a connection” to protect the end destination. These are fundamentally different.

For at least these reasons as well as the reasons provided in relation to claim 1, claims 6 and 7 are patentable over Beavers. Applicants respectfully request that the Examiner withdraw the rejection of claims 6 and 7.

In claim 13, as amended, Applicants claim a method comprising “determining a threat level associated with the connection request based at least in part on the static policy data attribute...and storing the threat level associated with the connection request as a dynamic policy data attribute in a dynamic policy data store” As discussed in relation to claim 1 above, Beavers does not disclose a method comprising “determining a threat level associated with the connection request based at least in part on the static policy data attribute...and storing the threat level associated with the connection request as a dynamic policy data attribute in a dynamic policy data store.” Thus Beavers does not anticipate claim 13, and Applicants respectfully request that the Examiner withdraw the rejection of claim 13.

Claims 14-17 depend from and further limit claim 13. Thus, claims 14-17 are patentable over Beavers for at least the same reasons as claim 13. Applicants respectfully request that the Examiner withdraw the rejection of claims 14-17.

III. Claims 3 and 4 under 35 U.S.C. § 103(a).

Claims 3 and 4 stand rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over Beaver in view of Avolio. In order to establish a *prima facie* case of obviousness, the reference must teach or suggest all of the claim limitations. See MPEP § 2143.

Claims 3 and 4 depend from and further limit claim 1. As discussed above, Beavers fails to teach or suggest all of the claim limitations of claim 1. Avolio is introduced as teaching that the severity of a threat is based upon the value of the object being secured. See Office Action, page 6. Thus, Avolio does not cure the deficiencies of Beavers, and claims 3 and 4 are patentable over Beavers in view of Avolio. Applicants respectfully request that the Examiner withdraw the rejection of claims 3 and 4.

IV. New Claim 20

Applicant has added new claim 20. Support for this claim can be found in the specification and the claims as originally filed. As in claim 1, in claim 20, Applicants claim “an authorization enforcement facility...operable to perform a risk-aware analysis of [a] connection to determine [a] threat level associated with the connection based at least in part on the static policy data attribute, and store the determined threat level in the dynamic policy data store as a dynamic policy data attribute.” Thus claim 20 is allowable for at least the reasons stated above in relation to claim 1.

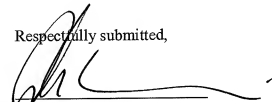
V. Conclusion

Applicants respectfully submit that all the currently pending claims are allowable. A favorable Office Action is respectfully solicited. The Examiner is invited to contact the undersigned at 336-607-7311 to discuss any matter related to the application.

Date:

July 21, 2008

Respectfully submitted,


John C. Alemanni
Registration No. 47,384

Kilpatrick Stockton LLP
1001 West Fourth Street
Winston-Salem, NC 27101-2400
Phone: 336-607-7311
Fax: 336-734-2621